TRIBUNAL SUPERIOR ELEITORAL

Informação nº 32 STI
Assunto: **Denúncia de acesso indevido de dados relativos aos sistemas eleitorais e ao projeto do *hardware* da UE2018**

Senhor Diretor-Geral,

1. Trata-se de informar acerca do recebimento de denúncia de acesso indevido de dados relativos aos sistemas eleitorais e ao projeto do *hardware* da UE2018. Tal denúncia foi encaminhada por *e-mail* à Assessoria de Comunicação deste Tribunal, a qual solicitou esclarecimentos sobre o teor do *e-mail* encaminhado pelo senhor Felipe Payão, identificado como repórter do portal TecMundo (https://www.tecmundo.com.br/). O conteúdo do *e-mail* encontra-se nos documentos anexos.

2. Com relação ao conteúdo do arquivo TSE.rar, encaminhado pelo repórter (conteúdo impresso anexo), é possível afirmar que:

2.1. foram incluídas capturas de tela de computador mostrando trechos de código-fonte do aplicativo Gedai-UE, de listas de arquivos e também de conteúdos de documentos; e
2.2. foram incluídos arquivos presentes na árvore de código-fonte do Gedai-UE.

3. Tal conteúdo evidencia o acesso indevido dos seguintes dados:
3.1. código-fonte completo do Gedai-UE, possivelmente da versão usada nas Eleições 2018, porém sem as assinaturas da Cerimônia de Lacração;
3.2. chaves e credenciais de acesso a servidores usadas pelo Gedai-UE;
3.3. senhas para oficialização dos sistemas Candidaturas e Horário Eleitoral utilizadas para a Eleição Suplementar 2018 de Aperibé/RJ;
3.4. manual técnico da impressora de votos desenvolvida pelo FIT/Quattro Eletrônica;
3.5. manual do QR Code do boletim de urna.

4. Não há evidência de acesso indevido do código-fonte do *software* da urna - Uenux, embora exista a evidência de acesso indevido de código comum entre o Gedai-UE e o Uenux.

5. Com relação ao material acessado indevidamente, o impacto é o seguinte:

5.1. o manual do QR Code (item 3.5) já é de domínio público e encontra-se publicado na Internet;
5.2. o manual da impressora de votos (item 3.4) não possui informação sensível, uma vez que trata-se da documentação de um protótipo que nunca entrou em

operação – o seu caráter sigiloso se deve a uma relação contratual entre o FIT e a Quattro Eletrônica;
5.3. as senhas de oficialização (item 3.3) permitem a alteração de dados de partidos e candidatos (até mesmo a sua exclusão) no contexto de um processo eleitoral (ou seja, no caso concreto afeta somente a Eleição Suplementar 2018 de Aperibé/RJ);
5.4 as credenciais de acesso aos servidores usadas pelo Gedai-UE (item 3.2) podem permitir que alguém dentro da intranet da Justiça Eleitoral consiga copiar os dados de eleitores e candidatos que alimentam as urnas, mas sem a capacidade de adulterá-los;
5.5. as chaves usadas pelo Gedai-UE (item 3.2) ainda requerem uma análise de risco mais detalhada; isso porque parte das chaves são geradas no momento da lacração e o acesso indevido diz respeito a material presente no ambiente de desenvolvimento – ou seja, o *software* lacrado usa chaves diferentes; na hipótese de serem as mesmas, existe a possibilidade de manipulação de arquivos de configuração que alimentam o *software* da urna; e
5.6. o código-fonte do Gedai-UE, acompanhado de seus binários compilados, permite a importação de dados oficiais das eleições e carregamento de urnas com esses dados; contudo, o *software* de urna utilizado não tem as assinaturas oficiais da lacração, o que fica evidenciado pelo LED de segurança da urna e pelos procedimentos de verificação de *hash* e assinatura; também não seria possível a geração de um boletim de urna válido para a Totalização a partir disso.

6. Diante desse cenário, solicita-se a abertura de inquérito policial junto à Polícia Federal para apuração dos fatos.

7. Outras providências já estão em andamento nesta STI para sanar as fragilidades que resultaram nesse acesso indevido, assim como tornar os sistemas expostos ainda mais seguros.

8. Finalmente, alerta-se sobre a necessidade de tramitação urgente deste processo.

É o que informo.

Brasília, 07 de novembro de 2018.

GIUSEPPE DUTRA JANINO
Secretário de Tecnologia da Informação